



(12) **EUROPEAN PATENT APPLICATION**

(43) Date of publication:
12.03.2003 Bulletin 2003/11

(51) Int Cl.7: **H04Q 7/32**, G06F 17/60,
H04L 29/06

(21) Application number: **01850152.8**

(22) Date of filing: **07.09.2001**

(84) Designated Contracting States:
**AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU
MC NL PT SE TR**
Designated Extension States:
AL LT LV MK RO SI

• **Dellmark, Jan**
184 60 Aekersberga (SE)
• **Arwald, Jan**
192 53 Sollentuna (SE)

(71) Applicant: **TELEFONAKTIEBOLAGET LM
ERICSSON**
126 25 Stockholm (SE)

(74) Representative: **Dahnér, Christer**
Ericsson Mobile Communications AB,
Patent Unit
164 80 Stockholm (SE)

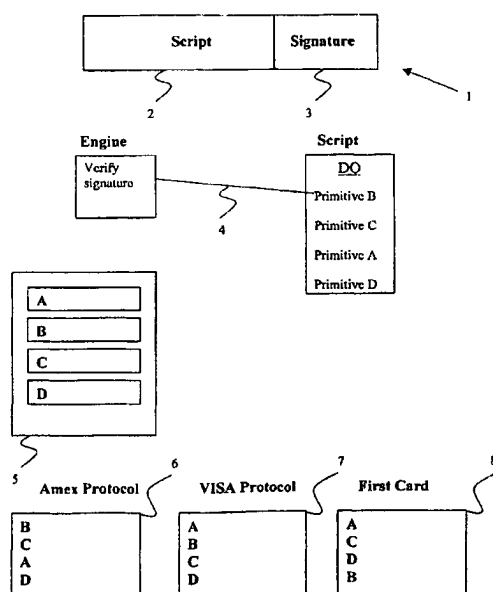
(72) Inventors:
• **Kiessling, Johan**
113 43 Stockholm (SE)

(54) **Method for adapting mobile terminals to different protocols and mobile terminal**

(57) A method for adapting mobile terminals in wireless communication systems to the variety of different protocols used when interacting with a multitude of different service providers. By using a set of building blocks, so called "primitives" stored in the terminal instead of having a set of protocols stored, a script is

downloaded from a service provider with instructions how the primitives should be arranged to form the desired protocol. The service provider secures his identity with a digital signature to ensure a correct operation. Preferably, the script is executed in one atomic operation. Preferably, the script forms a protocol adapted for money transactions.

FIG. 1



Description

TECHNICAL FIELD OF THE INVENTION

[0001] The present invention relates to a method for, and to a mobile terminal for, adapting mobile transceiving terminals in a wireless communication system to a variety of different protocols in a secure manner.

DESCRIPTION OF RELATED ART

[0002] In the emerging mobile electronic commerce, there is a need for implementing secure protocols for payments, tickets or other sensitive data. Today, a vast number of different protocols are used for similar applications. They have emerged from different industries as well as from different geographical areas.

[0003] Since the market for e-commerce still is so immature, it is likely to create a variety of new protocols over time. To cope with such an amount of protocols different solutions could be imagined and has also been proposed.

[0004] Until now, state of the art technique has proposed several alternatives to handle the large amount of different protocols. One solution has been to build in a subset of protocols in each mobile phone. This is not very successful since the numbers of protocols are too large to be implemented. Memory space is not an endless resource, especially not in mobile handsets when compared to PCs, and by this technique a lot of valuable memory will be used for services never wanted by the customer and also certain services that might be wanted has never been implemented. Also new protocols defined after the production of the mobile terminal can not be introduced.

[0005] Yet another problem is to deal with limited validity period of a protocol in a terminal. It also requires each service provider to evaluate and agree upon each step in production of the terminal to ensure the security of the implementation in each product.

[0006] Another solution would be to create an open area for application download. Unfortunately, the security may then be compromised due to viruses, false applications etc. downloaded to the mobile terminal. In the PC world of today, this is a very well known problem.

[0007] Yet another solution would be to build in protocols in an external device which could be used by the mobile terminal to download from. The obvious disadvantage with this method would be that your mobile terminal (commonly a mobile phone) will no longer be the center of mobile e-commerce. It would also require the user to carry around several gadgets and limit the number of users since not all mobile users are likely to have the extra device needed. The marginal costs would also be higher then compared to if it were implemented in an existing product like the mobile phone. An example of a product connected with this technique would be the "wireless wallet".

[0008] Still another technique that could be convenient would be to define a common mobile electronic transaction protocol. This seems hard to realize since that would require all industries using mobile transactions to agree on one single protocol. It would still not solve the problem with dynamic upgrades as a new version of the protocol is introduced. This would also require changes in existing infrastructure to accept the new protocol.

[0009] Therefore it would be desirable to be able to dynamically update the support for different protocols in individual terminals whilst preserving the high degree of security needed for electronic transactions.

SUMMARY

[0010] It is an object of the present invention to overcome the above mentioned problems and provide a method for adapting mobile terminals to different protocols in a wireless communication system overcoming all the above mentioned problems.

[0011] Another object of the present invention is to arrange for a transaction with full security and for which the user feels comfortable and safe when using.

[0012] According to one aspect of the present invention there is provided a method that enables a dynamical updating for different protocols as claimed in claim 1.

[0013] Instead of storing an excessive number of protocols in your mobile terminal, the idea underlying this invention is to store a number of primitives that, when put together, could form a script language in the terminal. The primitives could be characterized as the "building blocks" of the script language, i.e. the smallest identifiable units. The script language should then be used to form "scripts" that are able to describe a number of different protocols. A script could therefore be said to describe a selection of primitives following each other in a certain order to form a protocol.

[0014] These protocols should not be understood as restricted to mobile electronic transaction protocols even though such protocols will be used as example under the detailed descriptions.

[0015] The basic idea however, on which the invention relies, is that the primitives (building blocks) forming the protocols will have a longer lifetime themselves than the protocols they form. Protocols of today come and go, but their smallest units are often the same, arranged together in different orders. By securing the implementation of the primitives, different protocols can be utilized and thereby making the production of terminals less dependent of the service provisioning.

[0016] The script is preferably defined by a content or a service provider (such as VISA, AMEX or the local Certification Authority), which ensures that the script is to be trusted and that the protocol is valid.

[0017] To arrange for a transaction with full security the script is signed by a digital signature to ensure that no changes are made from the original definition of the

protocol. The signature will then be verified and the script executed in the terminal in a way that guarantees that the script is executed in one atomic operation by the calling application with the exact flow intended by the signer of the script.

[0018] A transaction method according to the invention thereby entails a number of advantages, e.g;

[0019] When you need to update a protocol you just have to update which primitives to use and in which order they should follow each other.

[0020] The primitives used are more stable over time than the more complex protocols built on top of them.

[0021] Implementations according to the invention allows dynamic download of complex protocols with full security and also automatically indicates to the user who is the issuer and are to be trusted.

[0022] The specific implementation in a given terminal can be hidden. If for example the protocol requires encryption based on minimum 64 bits, this can be implemented as for example SSL or WTLS in the transport layer. This would be transparent to the calling application as long as the encryption is supported by the terminal with at least the requested quality. Therefore neither the user, nor the service provider have to bother about hardware and software implementations in each terminal product to be used. Implementation dependencies irrelevant to the security are hidden in the primitives.

[0023] The primitives can be used to build any secure protocol, i.e. not limited to payments or tickets, as long as they can be described by a sequence of primitives.

BRIEF DESCRIPTION OF THE DRAWINGS

[0024] The features of the invention believed to be novel are set forth with particularity in the appended claims. The invention itself however, both as to organization and method of operation, together with further objects and advantages thereof, may be best understood by reference to the following description with the accompanying drawings, in the several Figures in which:

- Fig. 1 shows a block diagram depicting the basic structure and
- Fig. 2 shows a block diagram depicting a flow chart describing a preferred embodiment of the invention.

DETAILED DESCRIPTION OF EMBODIMENTS

[0025] In a preferred embodiment of the invention illustrated in Fig. 1 a set of primitives should be preloaded in a mobile terminal (e.g. mobile phone, smart phone or any computerized product with transceiving capability). These primitives could be simple commands that when put together form a script language.

[0026] Examples of such primitives are "Sign text", "Verify signature" or "Store copy protected". The primitives could also be mathematical algorithms or different

transactions towards a safe storage area on the phone, e.g. the SIM-card. Also primitives such as "If...Then", "While ... Do" are needed for flow control. By giving the primitives "labels", true identification standardization of the different primitives are ensured.

[0027] The script language is able to give a description for the primitives, in which order they should follow and how they should interconnect. It could also state the minimum quality required by each operation, (e.g. the key length needed for the encryption, whether personal keys/certificates need to come from smart cards or if a simple certificate in the RAM is enough)

[0028] The script language is then able to describe a number of different protocols. Such protocols could assist a user to perform a variety of services, e.g. mobile electronic transactions. Some scripts could be preloaded in the telephone, but the main advantage is evidently that a dynamical downloading of the script could take place when a user wants to start a certain application/transaction. The calling application will then just have to download the script needed for performing its task.

[0029] The script, which is defined by a company that acts as the service provider, should be signed with a digital signature to ensure that no changes are made from the original definition of the protocol.

[0030] This could e.g. be implemented so that a digital signature production part produces the digital signature using a secret key of the service provider which normally enciphers the data using an asymmetrical encipherment algorithm operating under both the secret and a public key. The digital signature is then added to the transmitting data of the script and is then transmitted to the mobile terminal. It can be deciphered using a complementary public key.

[0031] In that way the signature would be verified by the user and the script executed in the terminal as one atomic operation by the calling application. This ensures that the signer of the script, i.e. the company that acts as a service provider for the application, executes the script with the exact flow as intended. Hence it is very important that the script is not interrupted and that the user knows he is in contact with the service provider so there are no intermediate forgers.

[0032] The verification could be used as a criterion for displaying a security icon on the terminal. In that manner the user will be sure that a secure and correct operation is now available. The icon could e.g. be linked to the trademark of the company issuing/guaranteeing/signing the protocol, e.g. VISA or any other content provider.

The user is thereby informed that he is using a secure service and at the same time gets the verification of the content/payment provider. In this way no additional steps are needed from the user to get this verification. It also protects the service provider from false implementations.

[0033] Turning now to Fig. 1, the process is illustrated with an exemplary digital packet 1, containing information both about the script 2 and the digital signature 3.

This is just one example of a packet which could be downloaded to the mobile terminal from a service provider and the general concept of the invention is not to be restricted to any forms and kinds of digital packets.

[0034] The downloaded script 2 could be described as a recipe for creating a protocol out of primitives A-D. One of the primitives 4 could e.g. be the command "Verify signature". The engine running the script on the terminal could be certified to a certain capability of level and trust using code verification or other security mechanisms. Box 5 illustrates a secure storage for the primitives in the mobile terminal where access is only allowed after correct verification of the digital signature. By saying that the primitives should be stored in the mobile terminal, it is also implied that this could mean that they are stored on the SIM-card. Having them stored in the mobile terminal, (e.g. in a memory or on the SIM-card) is advantageous, but even having them stored in an external unit could be imaginable.

[0035] Box 6-8 represents three different protocols from three different imaginary service providers, where we see that the content of each protocol could differ in that the order of the primitives in each protocol differ.

[0036] Each primitive can be implemented in a variety of ways but the application can request a certain quality of service. For example that the certificate is stored on a smart card, that memory is copy protected, that the keyboard is tamper proof etc. Hence, the service quality requirements is decided by the application and secured by the digital signature. Each primitive and service quality level can be registered to indicate to an application on a higher level what options are available in a specific terminal at any given time.

[0037] A real case scenario example is presented in fig. 2;

[0038] A user 11 wants to perform a money transaction from one of his accounts to another. A mobile terminal 13 is used to connect to a server, e.g. via a WAP-browser 14. The server is under control of the service provider 12 (e.g. VISA). He selects the desired payment action 15 (here e.g. "transfer between own accounts") and sends a payment request to the service provider. The service provider determines what payment protocol is appropriate 16 and asks whether the protocol needed is already downloaded 17. The application checks if you already have the selected protocol,

i.e. if you are already a VISA customer. If not, the user can request a download of the protocol, whereby the service provider prepares the script, signs it and encrypts it with a private key 18. The script is then downloaded and the mobile terminal verifies and stores it 19.

[0039] The script is now ready for execution and that could start with a verification of the service provider signature 20 by using a public key according to any known technique. If verification is positive, the application could be set to display an icon, e.g. the Visa logo on the screen, to inform the user that it is a safe connection.

[0040] It could e.g. also be checked here that the prim-

itives used are primitives known by the mobile terminal so that the script is valid with reference to what the mobile terminal is prepared for.

[0041] The script could then e.g. include controlling of a PIN code 21,22 connected the user and, when considered ok by the service provider, allows the user to prepare the transaction 23. The user enters into his mobile terminal the transaction data (amount, account number etc.).

[0042] The transaction is signed 24 by the user using a private key and is sent 25 encrypted to the service provider. The transaction is now completed and the Visa-icon could be switched off 26.

[0043] This flowchart is merely imaginary exactly in what order commands are given and the stepwise procedures are executed. Variations in said flowchart lie within the scope of the invention and are only a simple software implementation design matter.

[0044] During the procedure and invisible to the user of the mobile terminal, the description of the protocol, the script, is downloaded. As mentioned above, the mobile terminal checks the digital signature according to any known technique by e.g. downloading a certificate or having a key already stored.

Claims

1. Method for adapting mobile terminals to different protocols in a wireless communication system **characterized in that** it enables a dynamical updating or downloading of different protocols by;

- defining a script language made of primitives, the script language being able to describe a variety of protocols, said primitives being stored in the mobile terminal
- downloading a script from a service provider into a mobile terminal, said script defining the order in which the primitives are to be executed, thus forming a protocol,
- executing said script in said mobile terminal.

2. Method for adapting mobile terminals to different protocols in a wireless communication system according to claim 1, characterized in that the service provider signs the script with a digital signature before the downloading into the mobile terminal.

3. Method for adapting mobile terminals to different protocols in a wireless communication system according to claim 2, characterized in that the execution of the script starts with a verification of said service provider signature.

4. Method for adapting mobile terminals to different protocols in a wireless communication system according to claim 2 or 3, **characterized in that** the

service provider signs the script using a private key and that the user verifies said signature using a public key.

5. Method for adapting mobile terminals to different protocols in a wireless communication system according to any of claims 2 to 4, **characterized in that** a correct verification is used as a criteria for displaying a security icon on the display of the mobile terminal. 5 10
6. Method for adapting mobile terminals to different protocols in a wireless communication system according to any of claims 1 to 5, **characterized in that** the script is executed in one atomic operation by the calling application. 15
7. Method for adapting mobile terminals to different protocols in a wireless communication system according to any of claims 2 to 6, **characterized in that** the calling application can request a certain quality of service level which will be secured by the digital signature. 20
8. Method for adapting mobile terminals to different protocols in a wireless communication system according to any of claims 1 to 7, **characterized in that** the downloaded script forms a protocol adapted for money transactions. 25 30
9. A mobile terminal used in a wireless communication system adapted to different protocols **characterized in that** it enables a dynamical updating or downloading of different protocols by storing a set of primitives, said primitives defining a script language being able to describe a variety of protocols and comprising; 35
- means for downloading a script from a service provider, said script defining the order in which the primitives are to be executed, thus forming a protocol and 40
 - means for executing said script. 45

50

55

FIG. 1

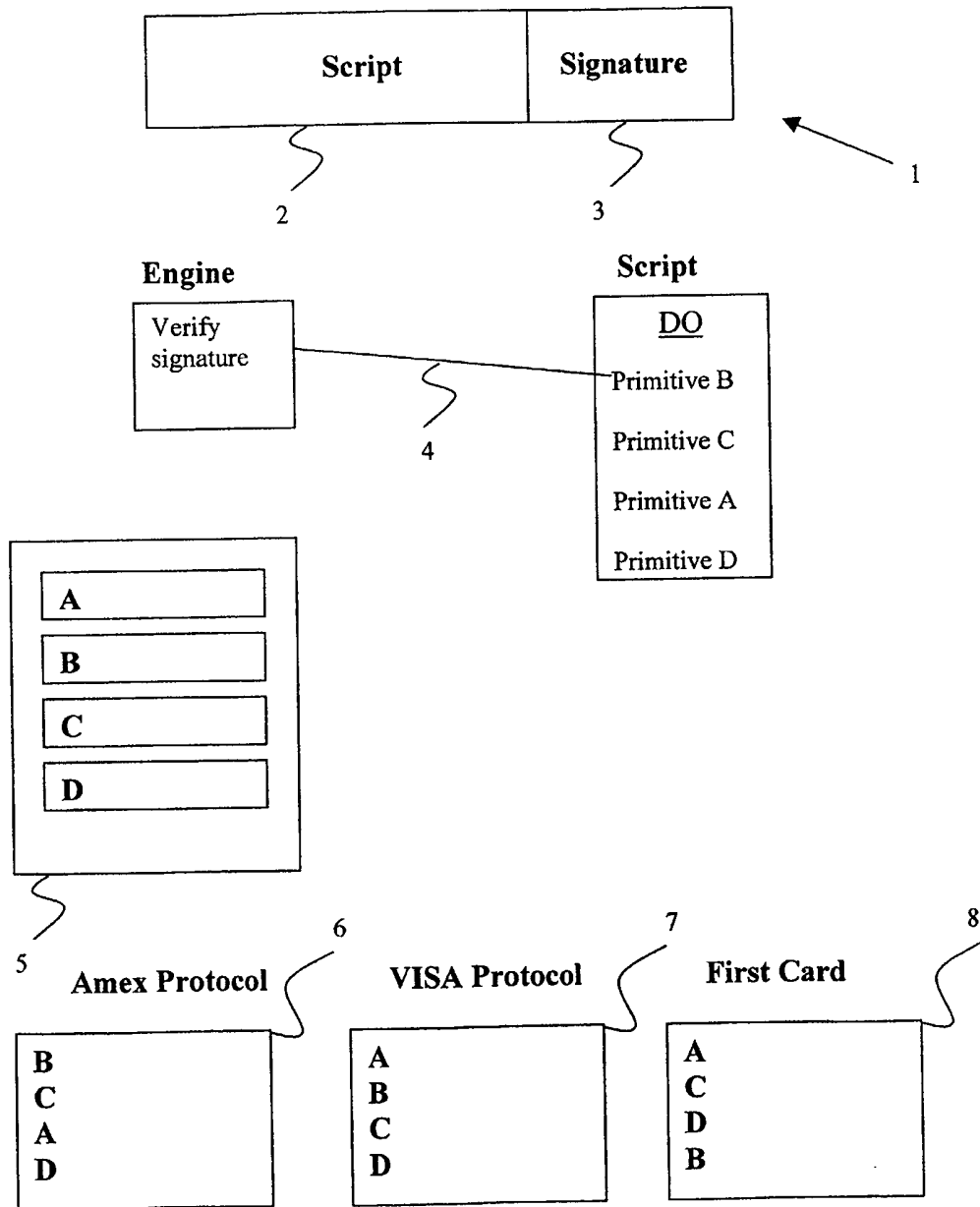


FIG. 2

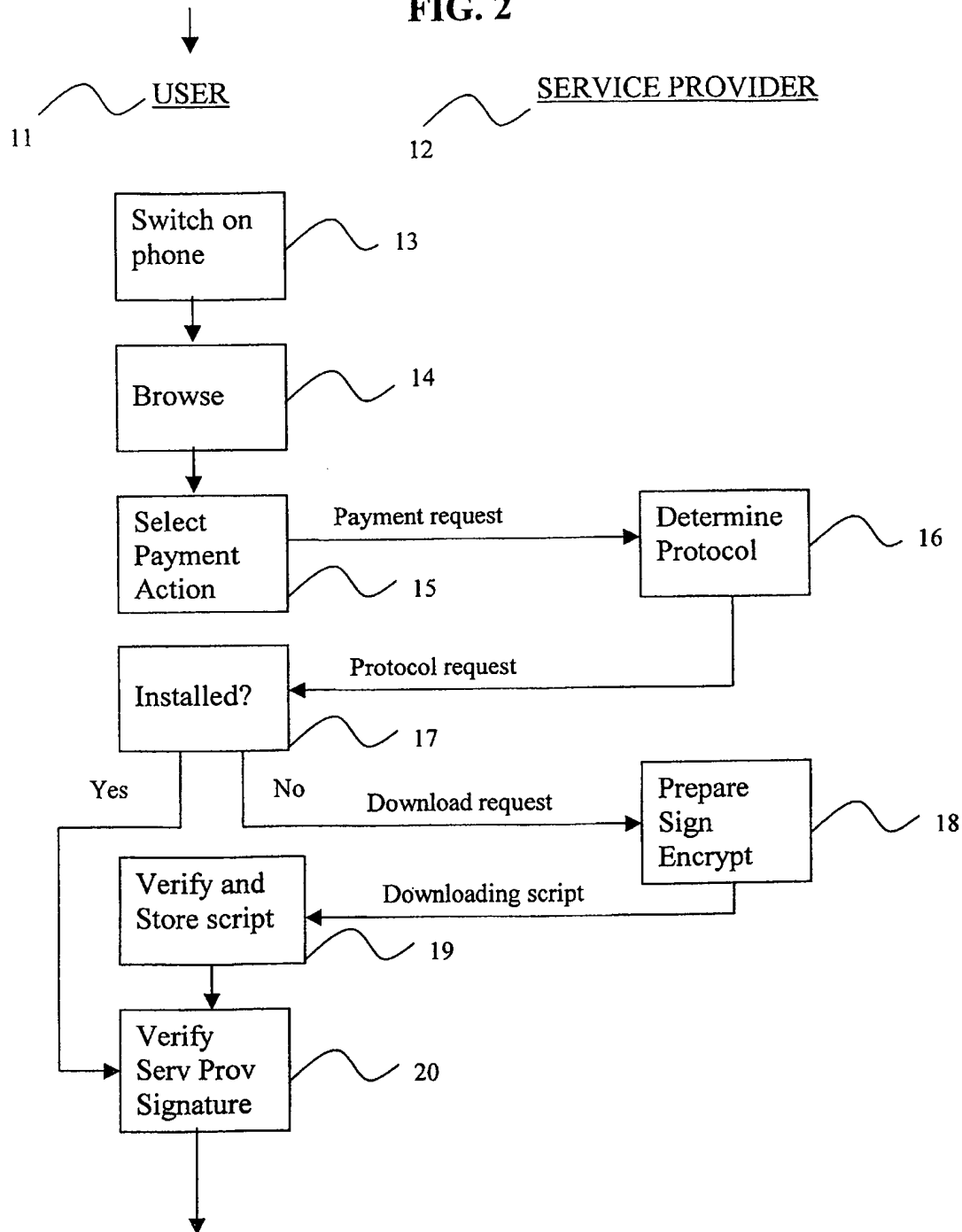
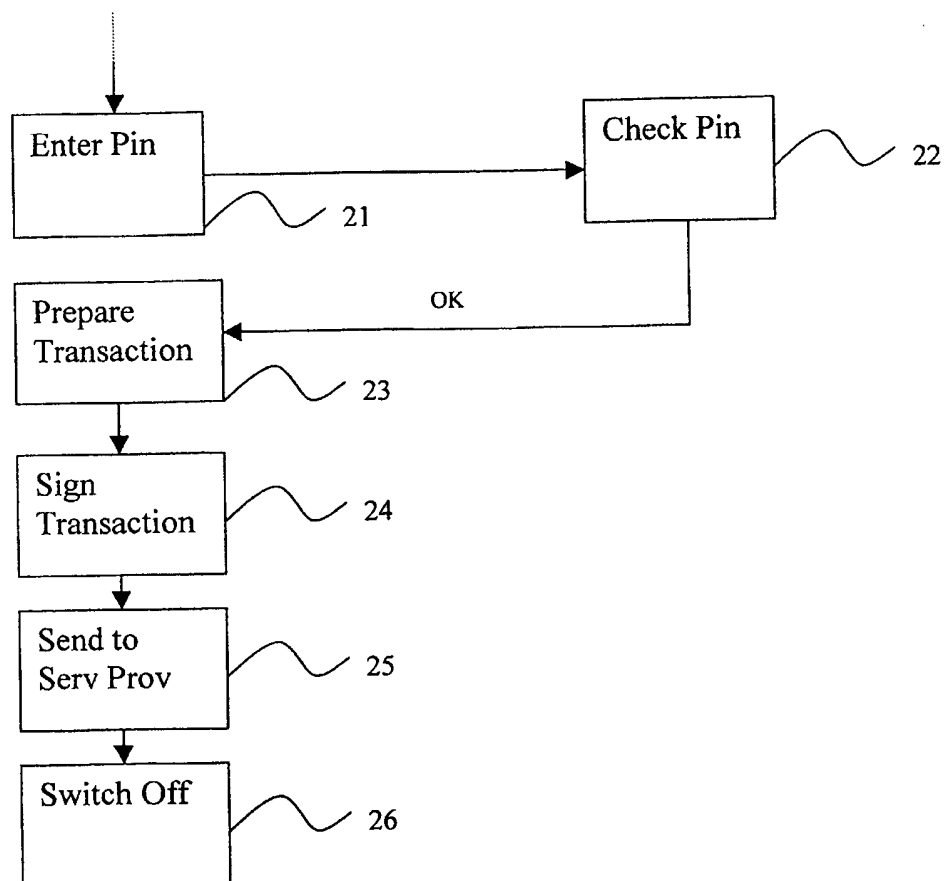


FIG. 2. cont.





European Patent
Office

EUROPEAN SEARCH REPORT

Application Number
EP 01 85 0152

DOCUMENTS CONSIDERED TO BE RELEVANT			
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
X	EP 1 033 652 A (NOKIA MOBILE PHONES LTD) 6 September 2000 (2000-09-06)	1-4,7-9	H04Q7/32 G06F17/60 H04L29/06
Y	* paragraph '0024! - paragraph '0027!; figure 3 *	5,6	
	* paragraph '0033! *		
Y	WO 01 50712 A (NOKIA CORP ;NOKIA INC (US)) 12 July 2001 (2001-07-12) * claim 8; figure 3 *	5	
X	WO 01 43472 A (SONERA OYJ ;VIRKKULA PETRI (FI); HEINONEN PETTERI (FI)) 14 June 2001 (2001-06-14) * page 12, line 21 - page 14, line 15 *	1-5,7,9	
Y	GB 2 335 568 A (NEC TECHNOLOGIES) 22 September 1999 (1999-09-22) * page 7, line 6 - line 11 *	6	
X	NOBLET C ET AL: "ASSESSING THE OVER-THE-AIR SOFTWARE DOWNLOAD FOR RECONFIGURABLE TERMINAL" IEE COLLOQUIUM ON PERSONAL COMMUNICATIONS IN THE 21TH CENTURY, IEE, LONDON, GB, 1998, pages 6-1-6-6, XP000668888	1,9	TECHNICAL FIELDS SEARCHED (Int.Cl.7) H04Q G06F H04L
A	Sections I and II "Introduction" and "The Over-the-Air Reconfiguration" * page 1 - page 3 *	2-8	
The present search report has been drawn up for all claims			
Place of search MUNICH		Date of completion of the search 25 January 2002	Examiner Köppl, M
<p>CATEGORY OF CITED DOCUMENTS</p> <p>X : particularly relevant if taken alone Y : particularly relevant if combined with another document of the same category A : technological background O : non-written disclosure P : intermediate document</p> <p>T : theory or principle underlying the invention E : earlier patent document, but published on, or after the filing date D : document cited in the application L : document cited for other reasons * : member of the same patent family, corresponding document</p>			

EPC FORM 1303 03.02 (P04CC1)

BEST AVAILABLE COPY

**ANNEX TO THE EUROPEAN SEARCH REPORT
ON EUROPEAN PATENT APPLICATION NO.**

EP 01 85 0152

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

25-01-2002

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
EP 1033652	A	06-09-2000	EP 1033652 A2	06-09-2000
			JP 2000347846 A	15-12-2000
WO 0150712	A	12-07-2001	AU 2211701 A	16-07-2001
			WO 0150712 A2	12-07-2001
WO 0143472	A	14-06-2001	FI 992661 A	11-06-2001
			AU 2375101 A	18-06-2001
			WO 0143472 A1	14-06-2001
GB 2335568	A	22-09-1999	AU 2124599 A	30-09-1999
			JP 11275215 A	08-10-1999
			US 6321079 B1	20-11-2001

BEST AVAILABLE COPY

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82